Malware | Emotet adds a further layer of camouflage | Spamhaus

Archived: 2026-04-02 11:58:27 UTC

Introduction

Most professionals within enterprise security have come across *'Emotet'*. As its history illustrates, the criminals behind Emotet malware are cunning and quick to maximize its 'potential.' From a basic banking Trojan to a threat distribution service, it is constantly being re-invented. This 'constant malware improvement' isn't showing any sign of abating. Recently the Spamhaus Malware Labs team have identified further unsettling changes in Emotet.

Emotet - what is it?

As previously mentioned, this malware came to the fore as a basic self-propagating banking Trojan in 2014. However, over the past 5 years the creators of this malware have taken the most successful facets of other disruptive software and created a modular malware family that can evade detection, spread like wildfire across a network and deliver multiple payloads.

Only a year ago Allentown, USA, hit the news headlines after becoming infected with Emotet. The remediation costs were reported to be in the region of US $1million.

Emotet - the data

In the last two months alone, the researchers at Spamhaus Malware Labs have tracked approximately 47,000 Emotet infected machines emitting around 6,000 distinct URLs to compromised websites serving as infection vectors. This makes Emotet the most actively distributed malware at the moment, accounting for almost 45% the total number of URLs used for this purpose.

There is no sign that the numbers associated with Emotet will decline over the forthcoming months, particularly given a recent discovery that will make Emotet even more difficult to detect.

Emotet HTTP advancement

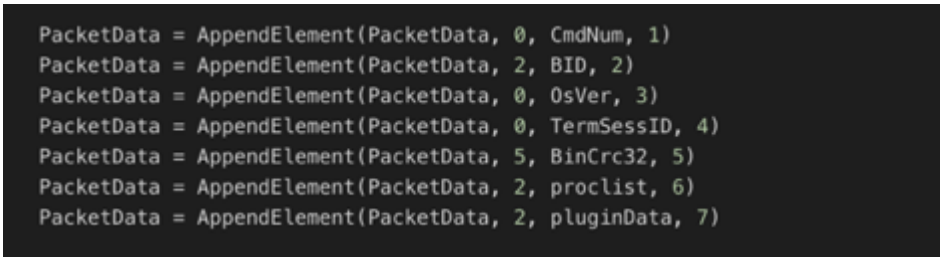
HTTP Headers - Previously, Emotet built moderately primitive HTTP packets. The fact they were primitive was a good thing; these HTTP packets didn't follow the standard protocol for either the type of data or how the data was sent. This made them easy to detect using a static signature on network traffic.

Unfortunately, these HTTP packets have become increasingly sophisticated: now they predominantly follow the RFC (Request for Comments) specifications of the HTTP protocol. These additional details in Emotet's HTTP

headers give the appearance of coming from a legitimate request, e.g., a browser or other application. As a result, a static signature on network traffic won't detect them, which is far from ideal.

Uniform Resource Identifier inclusion - Not only do we have the addition of these extra headers (as illustrated above), but Emotet has also started to include a Uniform Resource Identifier (URI). In the past, a URI was missing, but now it is randomizing between two different words. The URI randomly generates from a list of hardcoded comma separated words, as you can see in the example below.

It is worth noting that while Emotet's HTTP headers have changed the layer below, i.e., the custom protocol remains unchanged, as this image illustrates.



Protect yourself

The creators of Emotet have been savvy, and while nothing they have done is rocket science, there is clear evidence that they have a strong desire to make this malware more evasive and bulletproof. Which in turn means that you need to have bulletproof security.

Source: https://www.spamhaus.org/news/article/783/emotet-adds-a-further-layer-of-camouflage